Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

TA4903 Spoofing Government Entities and SMBs for Financial Gain

Date of Publication	Admiralty code	TA Number
March 8, 2023	A1	TA2024093

Summary

First Appearance: December 2021
Actor Name: TA4903
Target Industries: Government, Construction, Healthcare, Manufacturing, Energy, Finance, Agriculture, Transportation, Commerce, Food and Beverage
Target Region: United States of America

Actor Map

Actor Details

#1 TA4903 is a financially motivated cybercriminal group engaging in credential phishing and business email compromise (BEC) activities. They spoof U.S. government entities and various industries globally, targeting organizations primarily in the United States with high-volume email campaigns. Their main goals are to steal corporate credentials and conduct follow-on BEC activities.

#2 The group started spoofing U.S. government entities in 2021, expanding to departments like Agriculture, Transportation, and Commerce by 2023. They have also targeted small to medium-sized businesses across sectors such as construction, finance, healthcare, and others. TA4903 employs various tactics, including sending PDF attachments or URLs leading to phishing websites.

#3 In 2023, they began incorporating QR codes into PDFs and diversified their phishing themes to include references to confidential documents, ACH payments, and secure messages. They utilize actor-owned domain infrastructure and occasionally freemail addresses for delivering emails.

#4 Additionally, TA4903 employs EvilProxy, a multifactor authentication bypass tool, and has been observed conducting BEC campaigns with themes such as "cyberattacks" or "payment" to deceive recipients into providing sensitive information.

#5 Security researchers have observed instances of TA4903 using compromised credentials for follow-on BEC activities, such as invoice fraud, targeting the original victim's business partners and financial institutions. They also noted consistent traits in the group's tactics, such as domain construction, lure themes, and phishing kit usage.

#6 Overall, TA4903 remains a persistent threat, adapting their tactics to maximize their success in credential theft and BEC activities. Their recent shift towards BEC campaigns targeting small and medium-sized businesses suggests a potential evolution in their strategies or a temporary change in tactics.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
TA4903	Unknown **MOTIVE** Financial gain	United States of America	Government, Construction, Healthcare, Manufacturing, Energy, Finance, Agriculture, Transportation, Commerce, Food and Beverage

Recommendations

Email Filtering and Security: Implement robust email filtering solutions capable of detecting and blocking phishing emails before they reach users' inboxes. Utilize advanced threat protection features to identify malicious attachments, URLs, and spoofed sender addresses commonly used by TA4903.

Multi-Factor Authentication (MFA): Enforce MFA across all corporate accounts, especially for critical systems and applications like Office 365. MFA can significantly reduce the risk of unauthorized access, even if credentials are compromised through phishing attacks.

Domain Monitoring and Defense: Regularly monitor domain registrations for any suspicious activity or unauthorized variations of legitimate domains. Consider implementing domain-based message authentication, reporting, and conformance (DMARC) policies to prevent email spoofing and domain impersonation.

Endpoint Security: Deploy and maintain up-to-date endpoint security solutions to detect and prevent malware infections resulting from malicious attachments or links in phishing emails. Implement endpoint detection and response (EDR) solutions for real-time threat detection and incident response capabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0040 Impact
TA0006 Credential Access	TA0042 Resource Development	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1036 Masquerading	T1566.001 Spearphishing Attachment	T1566 Phishing	T1657 Financial Theft
T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File	T1566.002 Spearphishing Link
T1583 Acquire Infrastructure	T1111 Multi-Factor Authentication Interception		

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	ed4134de34fbc67c6a14c4a4d521e69b3cd2cb5e657b885bd2e8be0e45ad2bda, d398eef8cf3a69553985c4fd592a4500b791392cf86d7593dbdbd46f8842a18d, 15b9ae1ab5763985af2e6fe0b22526d045666609ad31829b8926466599eeb284, 6f776331d7c49ab6e403f84409c062db0b2027429e47e3533e8c6098c5f12156
Domains	orga-portal[.]com, Shortsync[.]net, index-dol[.]com
URLs	hxxps://auth01-usda[.]com, hxxp://tracking[.]tender-usdabids[.]com, hxxps://index-dolbid2024[.]com

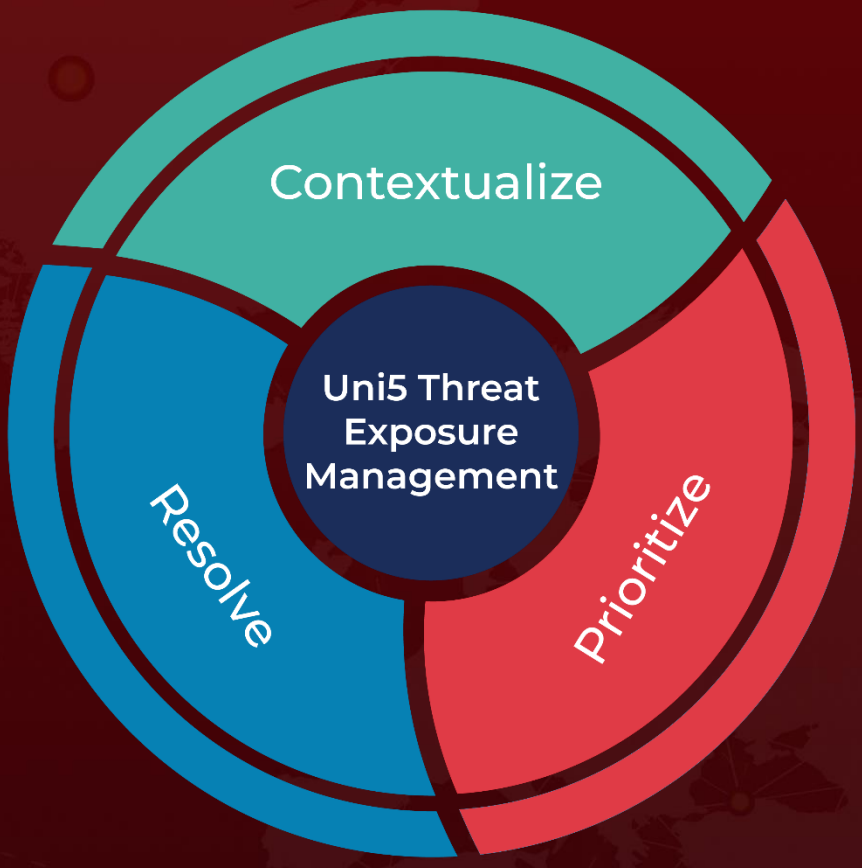
References

https://www.proofpoint.com/us/blog/threat-insight/ta4903-actor-spoofs-us-government-small-businesses-phishing-bec-bids

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 8, 2023 • 4:30 AM

More at www.hivepro.com